VZCZCXRO4708
OO RUEHAG RUEHAO RUEHAP RUEHAST RUEHAT RUEHBC RUEHBI RUEHBL RUEHBZ
RUEHCD RUEHCHI RUEHCI RUEHCN RUEHDA RUEHDBU RUEHDE RUEHDF RUEHDH
RUEHDT RUEHDU RUEHED RUEHEL RUEHFK RUEHFL RUEHGA RUEHGD RUEHGH RUEHGI
RUEHGR RUEHHA RUEHHM RUEHHO RUEHHT RUEHIHL RUEHIK RUEHJO RUEHJS RUEHKN
RUEHKR RUEHKSO RUEHKUK RUEHKW RUEHLA RUEHLH RUEHLN RUEHLZ RUEHMA
RUEHMC RUEHMJ RUEHMR RUEHMRE RUEHMT RUEHNAG RUEHNEH RUEHNG RUEHNH
RUEHNL RUEHNP RUEHNZ RUEHPA RUEHPB RUEHPD RUEHPOD RUEHPT RUEHPW RUEHQU
RUEHRD RUEHRG RUEHRN RUEHROV RUEHRS RUEHSK RUEHTM RUEHTRO RUEHVC
RUEHVK RUEHYG
DE RUEHC #9432/01 1602313
ZNR UUUUU ZZH
O 092251Z JUN 09
FM SECSTATE WASHDC
TO ALL DIPLOMATIC AND CONSULAR POSTS COLLECTIVE IMMEDIATE
RUEHTRO/AMEMBASSY TRIPOLI IMMEDIATE 7749

UNCLAS SECTION 01 OF 03 STATE 059432

SIPDIS

E.O. 12958: N/A
TAGS: EINT POLICY TINT SECURITY PREL PUBLIC RELATIONS
SUBJECT: PRESIDENT'S ROLLOUT OF THE 60-DAY CYBERSPACE POLICY REVIEW

¶1. (U) Posts are encouraged to use the press guidance and other information contained in Paragraph 3 below on the President's 60-day Cyberspace Policy Review to brief host governments and other. The U.S. Government anticipates working with foreign governments in bilateral and multilateral settings to advance our common interests in cybersecurity. Please report any interest on cybersecurity engagement and/or reaction to the rollout of the 60-day Cyberspace Policy Review by front channel cable, slugging your response for INR/CYBER. INR/CYBER coordinates within the Department through the Department's Cyber Policy Group (CPG).

¶2. (U) Background. The President has identified cybersecurity as one of the top priorities of his administration and directed an early 60-day, comprehensive review to assess U.S. policies and structures for cybersecurity. The review addressed all missions and activities associated with the information and communications infrastructure and the strategy will put a strong emphasis on collaboration with international partners across a range of issues.

(U) The President hosted an event on Friday, May 29th at the White House announcing the conclusion of the 60-Day Cyber Policy Review and endorsing the Review team's report. In addition to several Cabinet secretaries, representatives from the private sector, the Ambassadors from the UK, Canada, Australia and New Zealand; and representatives of the EU and the OAS were in attendance.

(U) The report includes a near-term action plan which recommends the appointment of a "cyber security policy official" based in the White House and responsible for coordinating the nation's cybersecurity policies and activities. A non-operational directorate, dual-hatted to the National Security and National Economic Councils, will be established under this official. Interagency coordination will occur primarily through the Information and Communications Infrastructure Interagency Policy Committee (ICI-IPC) and five sub-IPCs, including an International Sub-IPC. The Sub-IPCs will begin meeting immediately.

¶3. (U) Press Guidance. There will be a public web page for cybersecurity at
http://www.whitehouse.gov/cyberreview
which will include links to the 60-day report, submissions to the 60-day review by outside groups, streaming video from the President's speech, and videos from the Secretary of DHS among others discussing

cybersecurity issues.

(U)The White House issued the following Q&As drafted by the National Security Council and approved for the Press:

- What is meant when you use the term "Cybersecurity"?
-- ANSWER: As used in the Report the term "Cybersecurity" encompasses far more than simply taking preventative actions like patching computer systems. Cybersecurity broadly includes strategy, policy, and standards regarding the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military and intelligence missions as they relate to the security and stability of the global information and communications infrastructure.

- What are the next steps/priorities going forward?
-- ANSWER: The Report outlines an ambitious short- and mid-term action plan of vital tasks that must be addressed to help secure our information and communications infrastructure. This work will require both the coordinated effort of many federal departments and agencies and unprecedented partnership with the private sector, academia, state and local authorities, our international counterparts, and the public. Some of the key short-term tasks are: preparing an updated national strategy to secure the information and communication infrastructure; initiating a dialogue to

enhance public-private partnership, and initiating a national public awareness and education campaign to promote cybersecurity. We have much to do and it is a long road ahead, but we are on the right path and moving forward in an organized and comprehensive way.

- How are the actions outlined in the report different than the efforts in the last administration?
-- ANSWER: We are addressing the broad span of cybersecurity in a truly comprehensive way and designating it as a national priority so that we can achieve sustained long term success. No longer are we treating cybersecurity as a destination in itself, but instead understand that it is a compass that will guide our country to future economic growth and prosperity by providing a stable and secure foundation for commerce and communications. Though we are building on the progress made during the last administration, the scope and inclusiveness of our approach is far broader. Among other things, the President has designated a White House Cybersecurity Policy Official, who will be the center of gravity for cybersecurity issues. We are also committed to addressing other issues where progress is needed, including building a collaborative and workable public-private partnership, creating an effective cyber incident response plan, ensuring that foundational issues of infrastructure architecture incorporate security at the design stage, and substantially strengthening our strategic engagement with our foreign partners.

- What does this report mean for our international partners?
-- ANSWER: Cyberspace crosses international boundaries, and if we are to succeed in securing it we cannot act in isolation. The global challenge of securing cyberspace requires an increased effort to work with all countries-including those in the developing world who face these issues as they build their digital economies and infrastructures-plus international bodies, military

allies, and intelligence partners. This effort will seek-in continued collaboration with the private sector- to improve the security of interoperable networks through the development of global standards, expand the legal system's capacity to combat cyber crime, continue to develop and promote best practices, and maintain stable and effective Internet governance. The United States needs to develop a strategy designed to shape the international environment and bring like-minded nations together on a host of issues, including acceptable international norms that are critical to establishing a secure and thriving digital infrastructure. Accordingly, one of the priority short term actions identified in the Report is developing "U.S. Government positions for an international cybersecurity policy framework and strengthen our international partnerships to create initiatives that address the full range of activities, policies, and opportunities associated with cybersecurity."

- Australia, the U.K., Canada, France, New Zealand, and China all are working on or have announced cybersecurity strategies. Has the United States lost the chance to lead in this important area?
-- ANSWER: The fact that many countries around the world are recognizing the importance of cybersecurity is a positive step since this issue transcends national boundaries and requires unprecedented international cooperation. We have worked with many countries both in raising their awareness of this issue and exchanging information about how best to address it at a national and international level. The heightened importance that the President is giving to cybersecurity, including detailing an aggressive action plan that encompasses renewed international engagement, helps us and our closest allies continue to lead in this vital area.

- What is the scope of responsibility of the Cybersecurity Policy Official?
-- ANSWER: The Cybersecurity Policy Official - in consultation with the Federal government's Chief Technology Officer and Chief Information Officer and other offices including the office of Management and Budget, the Office of Science and Technology Policy and the National Economic Council - will harmonize cybersecurity-related policy and technology efforts across the Federal government, ensure that the President's budget reflects federal priorities for cybersecurity, and develop a legislative agenda for cybersecurity.

- What are the roles and responsibilities of the

Cybersecurity Policy Official?
-- ANSWER: The Cybersecurity Policy Official will coordinate interagency development of policies and strategies for the security of and operations in cyberspace that will help the United States achieve a more secure, reliable, resilient, and trustworthy digital infrastructure for the future. The Cybersecurity Policy Official will focus on harnessing the full benefits of innovation to address cybersecurity concerns and work on policies that address national security requirements, protection of intellectual property, and assuring the availability and continuity of infrastructure.

- If the United States suffers a major cyber attack tomorrow, who is in charge and how will we respond?
-- ANSWER: Ultimately, the White House is responsible for, and in charge of, high-level coordination during any major incident - including a major cyber incident. Many departments and agencies have important operational roles with respect to incident response, including the Departments of Homeland Security, Justice, and Defense

and the Intelligence Community, and each would continue to perform its operational roles in line with overall White House strategic direction.

- There are a lot of reports about other countries (e.g. Russia and China) attacking U.S. networks. Isn't the U.S. engaging in the same activity? What are we doing about these intrusions?
-- ANSWER: The cybersecurity threat is real and growing. Both foreign governments and criminals seek to exploit security holes in our government and private-sector networks to steal money and information and potentially to disrupt the networks themselves. Individual departments and agencies play various roles in securing government networks and investigating and prosecuting cyber crime. The cyberspace policy review surveyed U.S. government cybersecurity activities and developed action plans to build additional capabilities and to make government cybersecurity efforts more effective.

Minimize Considered.
CLINTON